

Security Incident Management Policy

Version Number	1.4
Data Classification	Internal (all employees have access)

	Name	Title	Signature	Date
Author	Emil Reisser-Weston	Data Controller		16/04/2021
Authoriser & Tested	Emil Reisser-Weston	Data Controller		16/04/2021

Issue Date	18/11/2019
Effective Date	16/04/2021
Review Date / frequency (check asset register)	21/11/2021

Version History

Previous version	Significant changes from previous version	Author	Date
1.0	Added Procedure for Reporting Incidents	Alan Thomas	18/11/2019
1.1	Checked - information added re Power Outage and continuity and how it affects security. Reference to Apprentix removed	Emil Reisser-Weston	01/07/2020
1.2	Updated with references to Jira over old system: Bitbucket. Updated warning categories.	Emil Reisser-Weston	21/11/2020
1.3	Added procedures regarding Collecting Evidence		16/04/2021

THIS IS A CONTROLLED DOCUMENT. DO NOT COPY UNLESS FOR ARCHIVING PREVIOUS VERSION

Contents

1 Policy Statement	4
2 Purpose	4
3 Scope	4
4 Definition	4
5 Risks	5
6 Procedure for Incident Handling	5
6.1 Jira Reporting	5
6.2 Line Manager Reporting	6
6.3 Client Notification	7
7 Procedure for Recording Events & Incidents	7
7.1 Reporting the Event/Incident	7
7.2 Classifying the Event/Incident	8
7.3 Collecting Evidence	8
8 Procedure for Power Outage	9
9 Policy Compliance	10
10 Policy Governance	10
11 Review and Revision	11
12 Key Messages	11

1 Policy Statement

eLearning WMB will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems supplied by the company - this relates mostly to the Open eLMS system (including the SMCR Solution.).

2 Purpose

The aim of this policy is to ensure that eLearning WMB reacts appropriately to any actual or suspected security incidents relating to information systems and data.

3 Scope

This document applies to all employees of eLearning WMB including contractual third parties and agents of the company who assist with the implementation of the company's systems, or support them after installation.

4 Definition

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an "information management security incident" in the remainder of this policy and procedure is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and/or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (successful or otherwise) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without eLearning WMB's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix 2.

5 Risks

eLearning WMB recognises that there are risks in its staff accessing client data for the purposes of installation, setup, support and maintenance of the underlying Open Elms and related systems.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of eLearning WMB and the trust that the company's customers place in the organisation, and may result in financial loss and the loss of future business.

6 Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by an Information Security Team - this consists of the Head of IT and the Data Controller at eLearning WMB.

Should this reporting directly concern the computer systems supplied by eLearning WMB (Open Elms, SMCR Solution etc.) then this should be reported directly using the Jira incident management system.

Should the incident concern the deliberate misuse of company information for malicious purposes or otherwise, then this should be reported directly to each employee's line manager.

6.1 Jira Reporting

All staff are trained in the use of the Jira incident reporting system.

All **suspected** security issues are raised as Bugs, and get the highest priority - they are given a priority as either Trivial, Minor, Major, Critical or Blocker - these priorities align to an estimate of the risk level being Low, Low Medium, Medium, Medium High or High.

Other kinds of issues should be labeled as below - the targeted percentage proportion of each issue is demonstrated along with the estimated time for which they will be resolved.

Severity	Target Population	Response time	Resolution target
Blocker	5%	1 working hour	2 working hours
Critical	20%	1 working hour	4 working hours

Major	50%	2 working hours	2 working days
Minor	20%	1 working day	4 working weeks
Trivial	5%	5 working days	1-30 working weeks

All suspected incidents are then assigned to the Data Controller who, after consultation with the Head of IT and relevant stakeholders, assign the task for resolution and confirm or change the priority. The Data Controller will also be responsible for informing the client of any breaches should it be of concern.

The program team will work through issues rated in line with priority. Once the program team is satisfied, the issue will have its status changed to “Resolved”. The Data Controller will check that the issue is resolved in line with security requirements with the assistance of the Head of IT. Once this is done, the issue will be further checked against a user story test case and annotated accordingly, if necessary.

6.2 Line Manager Reporting

Examples of incidents which would involve reporting to a line manager (in effect this would be the “Project” or “Product Manager”) are listed below. These incidents would be discussed with the Data Controller to see if there are further actions to take (such as informing any affected parties and changing procedures) and to see if alterations are needed to the company’s overall security arrangements and risk management procedures.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer or USB key infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff' by mistake.
- Responding to an email Phishing attack.
- Unknown people asking for information which could gain them access to a client’s data (e.g. an admin password).

Misuse

- Use of unapproved or unlicensed software on eLearning WMB equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down password information and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file. Theft / loss of any computer equipment containing client data

6.3 Client Notification

When an incident is identified which has a significant effect (either the incident itself or steps taken to resolve the incident) upon the client's system, the client's main contact should be notified within the same business day. All client main contacts are stored in the Hubspot client database - access is available to key security personnel and the respective account manager of each client.

Failure to notify clients under such circumstances is a disciplinary offense.

Examples of major incidents which require notification include, but are not limited to:

- The service is taken down during business hours (Monday to Friday 8.30am to 5.30pm) for a duration of longer than 3 minutes
- The service is taken down for outside business hours (Monday to Friday 8.30am to 5.30pm) for a duration of longer than 10 minutes
- There has been a malicious attack of any kind on a client's site
- A security breach has been identified which could lead to a client's admin password being exposed
- A security breach of a client's Personal Identity Information which could lead to the unauthorised exposure of that information to third-parties.
- The deletion of client data

7 Procedure for Recording Events & Incidents

In line with the company's commitment to data security and compliance with certifications such as ISO27001, all events, incidents, near misses or suspected weaknesses must be properly recorded for audit and improvement purposes.

If you have become aware of any event connected to security, you should first report it to the relevant person (Data Controller) and then complete an entry in the [Incident Log](#) (part of the asset register).

7.1 Reporting the Event/Incident

Complete the columns as follows:

- 1. No.**
This is the incident number - column should be populated already, if not continue numbering based on row above.
- 2. Date**
Date of log entry
- 3. Asset No.**
Find the affected asset within the Asset Register - use the asset ID number assigned for the log.
- 4. Is breach information related?**
Based upon where the breach occurred, could there have been unauthorised access to information? Answer Yes or No.

5. Information Classification

What was the classification status of the data BEFORE the breach occurred?
(Confidential/Restricted/Internal/Public) - see [Information Classification Policy](#).

6. Severity

Enter a number between 1 - 5 where 1 = LOW /3 = MEDIUM /5 = HIGH

7. Description of Incident

Include all relevant information you can gather about the incident in this column, including:

- Date of the breach itself (if known)
- The affected systems and/or resources
- How was it detected?
- What are the impacts?
- How did it happen? Are vulnerabilities known?
- Which (if any) clients will be affected?
- Estimated time to rectify

8. Remedial Action

Based upon the previous column, what needs to be changed to prevent a similar incident from happening again?

9. Reported By

Your name

7.2 Classifying the Event/Incident

‘Events’ are incidents with a low Severity (1) and are often planned tasks which although affect security, they have often been scheduled or predicted and procedures have been put in place to drastically reduce any effect they would have on the security of information within the company.

The Data Controller is responsible for this process and will check each issue and colour code events in green as part of management of the log. Only the data controller has rights to do this, although their will often be collaboration with other parties before deriving any decision.

7.3 Collecting Evidence

Should a breach occur, it may be necessary to get outside contractors in to gather evidence to support any claim or derive the source of any errors in the Information Security Management System so improvements can be made.

In such cases it is important that the digital landscape remains as unchanged as possible so a specialist firm involved in digital forensics can investigate further. eLearning WMB employees as a result have to ‘secure the scene’ by taking the following steps:

Don’t change any data

If anyone does anything that results in the data on the relevant system being altered in any way then this will affect any subsequent court case etc. Examples could be as simple as waking up a laptop or logging on. So think before you touch anything.

Only access the original data in exceptional circumstances

The first thing a specialist will do is use some tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or maybe a SIM card on a phone. All analysis then takes place on the copy and the original is never touched unless maybe time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible (this is rare).

Keep an audit trail

Always keep an audit trail of what has been done. Forensic tools will do this automatically but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as you don't touch anything to do it.

Ensure guidelines are followed

eLearning WMB's Data Controller will ensure that these guidelines are followed. Few excuses are accepted in court, so it is essential that staff are made aware on how to respond.

8 Procedure for Power Outage

In the event of a power outage within any computing facilities, the guidelines and procedures in this section are to be followed.

Procedure

STEP	ACTION
1	Assess the situation and determine if outside assistance is needed; if this is the case, dial 999 immediately.
2	Immediately notify all other personnel in the facility of the situation and be prepared to cease voice operations accordingly.
3	Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly.
4	A power outage may have different causes: • DO NOT under any circumstances attempt to repair or otherwise access electrical systems that you are not qualified to handle. • If there is no immediate danger, contact Sorbon Estates: ○ Lee Scowen - 01494 683823 ○ Melanie Wills - 01494 683857

9 Policy Compliance

If any user is found to have breached this policy, they may be subject to eLearning WMB's disciplinary procedure. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Advice concerning the implications of this policy or how it may apply can always be sought from the Data Controller.

10 Policy Governance

The following table identifies who within eLearning WMB is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Data Controller
Accountable	Data Controller, Head of IT
Consulted	The company board
Informed	All Employees, stakeholders and contractors

11 Review and Revision

This policy, and all related appendices, will be reviewed every 12 months, or sooner should the need arise..

Policy review will be undertaken by the Data Controller.

12 Key Messages

- All staff should report any incidents or suspected incidents immediately by the Jira system and then if it is a true security incident, in the [Incidents Log](#)
- All incidents then become the responsibility of the Data Controller
- All incidents related to security are prioritised
- Consult the Data Controller if you are unsure of anything in this policy